Report No. DODIG-2016-075

~~FOR OFFICIAL USE ONLY Law Enforcement Sensitive~~

INSPECTOR GENERAL

U.S. Department of Defense

APRIL 25, 2016

Evaluation of the Air Force Office of Special Investigations' Conduct of Internet-Based Operations and Investigations

~~***LAW ENFORCEMENT SENSITIVE:*** *The information in this document marked FOUO-LES is the property of DoD OIG and may be distributed within the Federal Government (and its contractors) to law enforcement, public safety and protection, and intelligence officials and individuals with a need to know. Distribution to other entities without prior DoD OIG authorization is prohibited. Precautions shall be taken to ensure this information is stored and destroyed in a manner that precludes unauthorized access. Information bearing the FOUO-LES marking may not be used in legal proceedings without prior authorization from the originator. Recipients are prohibited from posting information marked FOUO-LES on a website or unclassified network.*~~

~~*Safeguard this report and do not show or release its contents for other than official review and comments. Do not disclose its contents outside your DoD Component.*~~

INTEGRITY ★ EFFICIENCY ★ ACCOUNTABILITY ★ EXCELLENCE

~~The document contains information that may be exempt from mandatory disclosure under the Freedom of Information Act.~~

~~FOR OFFICIAL USE ONLY Law Enforcement Sensitive~~

INTEGRITY ★ EFFICIENCY ★ ACCOUNTABILITY ★ EXCELLENCE

Mission

Our mission is to provide independent, relevant, and timely oversight of the Department of Defense that supports the warfighter; promotes accountability, integrity, and efficiency; advises the Secretary of Defense and Congress; and informs the public.

Vision

Our vision is to be a model oversight organization in the Federal Government by leading change, speaking truth, and promoting excellence—a diverse organization, working together as one professional team, recognized as leaders in our field.

For more information about whistleblower protection, please see the inside back cover.

Results in Brief

Evaluation of the Air Force Office of Special Investigations' Conduct of Internet-Based Operations and Investigations

April 25, 2016

Objective

We evaluated the Air Force Office of Special Investigations' (AFOSI) conduct of Internet-based operations and investigations initiated during the period of January 2010 through October 2014. We evaluated the procedures used to initiate and participate in Internet-based operations and investigations with Federal, state, and local law enforcement agencies' Internet crimes task forces.

Specifically, we focused on whether AFOSI had adequate:

- policy and guidance governing Internet-based operations and investigations; and
- policies and procedures for its special agents' participation in operations such as Internet Crimes Against Children (ICAC).

Finding

AFOSI lacked specific policy addressing its special agents' roles during ICAC operations, which contributed to violations of the provisions in DoD Directive (DoDD) 5525.5, "DoD Cooperation with Civilian Law Enforcement Officials," and the DoDD's revised version, DoD Instruction (DoDI) 3025.21, "Defense Support of Civilian Law Enforcement Agencies." These violations were the result of AFOSI special agents participating in prohibited investigative activities with civilian law enforcement agencies before establishing a reasonable likelihood of a subject's military affiliation. During our evaluation, AFOSI published investigative policy, which incorporated the reasonable likelihood standard and provided guidance and clarity regarding ICAC operations. In addition, DoDI 3025.21 has not been updated to include the reasonable likelihood standard articulated in *United States v. Dreyer*, 767 F.3d 826 (9th Cir. 2014).

Finding (cont'd)

Of 80 AFOSI cases we reviewed, 23 (29 percent) lacked a reasonable likelihood of the subject's military affiliation. In those 23 cases, AFOSI special agents participated in prohibited investigative activities in violation of DoDD 5525.5, DoDI 3025.21, and AFOSI Manual 71-118, volume 3, "Undercover Operations." Special agents violated policy by conducting criminal investigations without first establishing a reasonable likelihood of the subject's military affiliation.

Observation

At the time of the evaluation, AFOSI policy did not clearly define special agents' roles and responsibilities regarding Internet-based operations nor did it require the execution of memorandums of understanding for participation in ICAC task forces. However, during the course of our evaluation, AFOSI revised its policy and it now provides clear guidance governing its agents' participation in ICAC operations.

Recommendation

We recommend that the Under Secretary of Defense for Policy clarify DoD Instruction 3025.21, enclosure 3, to reflect the holding in *United States v. Dreyer*, 767 F.3d 826, affirmed in relevant part by 2015 U.S. App. LEXIS 19226 (9th Cir., *en banc*). *Dreyer* established a standard requiring a reasonable likelihood of a subject's military affiliation before Military Criminal Investigative Organizations (MCIOs) conduct investigative activities.

Management Comments and Our Response

The Director, Defense Support of Civil Authorities, responding for the Under Secretary of Defense for Policy, agreed with our recommendation, but stated that the Dreyer violation was more of an education and training issue than a policy issue. However, we believe it is more than a training issue and feel clarification of the Instruction is appropriate. We also request that the Under Secretary of Defense for Policy provide a response on what additional training and education will be provided, and when that will occur.

Recommendations Table

Management	Recommendations Requiring Comment	No Additional Comments Required
Under Secretary of Defense for Policy	1	

Please provide Management Comments by May 25, 2015.

INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
4800 MARK CENTER DRIVE
ALEXANDRIA, VIRGINIA 22350-1500

April 25, 2016

MEMORANDUM FOR UNDER SECRETARY OF DEFENSE FOR POLICY
ASSISTANT SECRETARY OF THE AIR FORCE
(FINANCIAL MANAGEMENT AND COMPTROLLER)

SUBJECT: Evaluation of the Air Force Office of Special Investigations' Conduct of Internet-Based Operations and Investigations (Report No. DODIG-2016-075)

We evaluated the procedures used by the Air Force Office of Special Investigations (AFOSI) to initiate and participate in Internet-based operations and investigations with Federal, state, and civilian law enforcement agencies' Internet crimes task forces. The overall objective was to determine whether the AFOSI had sufficient policy guidance and supervisory oversight governing Internet-based operations such as Internet Crimes Against Children (ICAC). We conducted this evaluation in accordance with the Council of Inspectors General on Integrity and Efficiency, "Quality Standards for Inspection and Evaluation."

We determined that AFOSI lacked specific policy addressing its special agents' roles during ICAC operations, which contributed to violations of the provisions in DoD Directive (DoDD) 5525.5, "DoD Cooperation with Civilian Law Enforcement Officials," and the DoDD's revised version, DoD Instruction (DoDI) 3025.21, "Defense Support of Civilian Law Enforcement Agencies." These violations were the result of AFOSI special agents participating in prohibited investigative activities with civilian law enforcement agencies before establishing a reasonable likelihood of a subject's military affiliation. We also determined DoDI 3025.21 has not been updated to include the reasonable likelihood standard articulated in *United States v. Dreyer*, 767 F.3d 826 (9th Cir. 2014). We observed AFOSI policy did not clearly define special agents' roles and responsibilities regarding Internet-based operations nor did it require the execution of memorandums of understanding for participation in ICAC task forces. However, during the course of evaluation, AFOSI revised its policy and it now provides clear guidance governing its agents' participation in ICAC operations.

We considered management comments on a draft to this report when preparing the final report. The Director, Defense Support of Civil Authorities agreed with our recommendation to clarify DoDI 3025.21, enclosure 3, to reflect the holding in *U.S. v. Dreyer* when it revises the instruction sometime in 2017. However, the Director stated the Dreyer violation was more of an education and training issue than a policy issue. We disagree and request that the Under Secretary of Defense for Policy reconsider his position and provide comments in response to the final report. Comments are required by May 25, 2016.

Portions of this report are marked "Law Enforcement Sensitive" (FOUO-LES) to prevent the disclosure of law enforcement tactics, techniques, and procedures. While some of the data contained in those sections may be a matter of public record, it is not widely publicized and the source document for the information is a Department of Justice product that was similarly classified.

We appreciate the courtesies extended to our staff. Please direct any questions to Supervisory Special Agent [redacted]. If you desire, we will provide a formal briefing on the results.

Randolph R. Stone
Deputy Inspector General
Policy and Oversight

cc:
Secretary of the Air Force/Inspector General, Director of Special Investigations
Commander, Air Force Office of Special Investigations

Contents


INSPECTOR GENERAL
INTEGRITY
EFFICIENCY
DEPARTMENT OF DEFENSE

Introduction

Objective

Our objective was to evaluate the Air Force Office of Special Investigations' (AFOSI) conduct of Internet-based operations and investigations. For this evaluation, Internet-based operations and investigations are (a) investigations involving the peer-to-peer (P2P) transfer of computer files containing child pornography and (b) investigations concerning the use of the Internet for solicitation of a minor (under the age of consent) for sexual purposes. We evaluated the procedures used to initiate and participate in Internet-based operations and investigations with Federal, state, and local law enforcement agencies' Internet crimes task forces. Specifically, we focused on whether AFOSI had adequate:

- policy and guidance governing Internet-based operations and investigations and
- policies and procedures for its special agents' participation in operations such as Internet Crimes Against Children (ICAC).

See the Appendix for our scope and methodology.

Background

Figure 1. Internet Crimes Against Children Logo
Source: Internet Crimes Against Children Task Force Program

The DoD Office of Inspector General (OIG) initiated this evaluation to examine AFOSI's involvement with, or support to, civilian law enforcement agencies in the realm of the investigation of P2P file transfers of child pornography and the solicitation of minors for sexual purposes. We evaluated the procedures used to initiate and participate in Internet-based operations and investigations with Federal, state, and civilian law enforcement agencies' ICAC task forces. We determined whether AFOSI has sufficient policy guidance and supervisory oversight governing Internet-based operations and to determine whether AFOSI is complying with the Posse Comitatus Act as implemented by DoD policy.

The ICAC Program is a national network of 61 coordinated local task forces and nearly 3,000 local and regional-affiliated agencies engaged in both proactive and reactive investigations, forensic examinations, effective prosecutions, and community education. The ICAC Program was developed in response to the

increasing number of children and teenagers using the Internet, the proliferation of unlawful images, contraband images, images depicting the sexual exploitation of minors, and the heightened online activity by predators searching for unsupervised contact with underage victims. By helping civilian law enforcement agencies develop effective and sustainable responses to online child victimization and unlawful images, contraband images, and images depicting the sexual exploitation of minors, the ICAC program delivers national resources at the local level.

Federal Law

The "Posse Comitatus Act" (18 U.S.C. §1385) generally prohibits the use of military personnel to enforce civilian law. In addition, 10 U.S.C. §§ 371 - 382 contains guidance on how, when, and under what circumstances the military can be used to support civilian law enforcement agencies.

Section 375, title 10, United States Code (10 U.S.C. §375) requires the Secretary of Defense to issue regulations:

> as may be necessary to ensure that any activity (including the provision of any equipment or facility or the assignment or detail of any personnel) under this chapter does not include or permit direct participation by a member of the Army, Navy, Air Force, or Marine Corps in a search, seizure, arrest, or other similar activity unless participation in such activity by such member is otherwise authorized by law.

Sections 371 - 382, title 10, U.S.C. further clarifies that the referenced activity will not result in use of the armed forces to make arrests or conduct searches and seizures solely for the benefit of civilian law enforcement. Furthermore, 10 U.S.C. §371 authorizes military law enforcement personnel to provide information collected during the normal course of military training or operations that may be relevant to a violation of any Federal or State law to the appropriate civilian law enforcement officials.

United States v. Dreyer

In September 2014, a three-judge panel of the 9th Circuit Court of Appeals handed down a decision in *United States v. Dreyer*, 767 F.3d 826 (9th Cir. 2014). The decision addresses, in reference to Internet-based investigations, the application of the Posse Comitatus Act and Posse Comitatus Act-like restrictions imposed by 10 U.S.C. §375 and DoD regulations that implement the Act. The *Dreyer* opinion articulated a "reasonable likelihood" standard with regard to any investigative activities undertaken in reliance on the "independent military purpose" exception to the limitations imposed by the Posse Comitatus Act, the Posse Comitatus Act-like restrictions imposed by 10 U.S.C. §375 and the associated DoD regulations.

Specifically, in order to bring the investigative activity within the scope of the "independent military purpose" exception, the Military Criminal Investigative Organization (MCIO) must show that there was a reasonable likelihood that the subject of the investigation had a military affiliation before the MCIO undertook specific investigative activity.

Specifically, the *Dreyer* opinion stated:

> the Ninth Circuit held that a Naval Criminal Investigative Service (NCIS) special agent who launched a broad investigation into the sharing of child pornography on a peer-to-peer network by anyone in the State of Washington violated policies and regulations restricting military participation in civilian law enforcement activities. In this case, the special agent's efforts identified a resident within the state of Washington that had no military affiliation.[*Dreyer* at 831-832.]
>
> The court found that the special agent had not adequately attempted to limit his search to members of the military and therefore his investigation did not serve an independent military function. [*Dreyer* at 835.]

In short, based on the holding in *Dreyer*, investigations conducted by MCIOs must have a reasonable likelihood of a military affiliation to ensure compliance with statutes and policy.

In November 2015, the 9th Circuit, siting *en banc*, affirmed the portion of the earlier 9th Circuit panel's decision that a violation of the Posse Comitatus Act-like restrictions on direct assistance to civilian law enforcement had occurred based on the fact that the investigation did not fall within the parameters of the "independent military purpose" exception to the Posse Comitatus Act, *United States v. Dreyer*, 2015 U.S. App. LEXIS 19226.

DoD Policy

DoD personnel were prohibited (where no exception existed) by DoD Directive (DoDD) 5525.5, "DoD Cooperation with Civilian Law Enforcement Officials," enclosure 4, January 15, 1986, (Incorporating Change 1, December 20, 1989) from participating in the following forms of direct assistance to civilian law enforcement:

- interdiction of a vehicle, vessel, aircraft, or other similar activity;
- a search or seizure, an arrest, apprehension, stop and frisk, or similar activity; and
- surveillance or pursuit of individuals, or as undercover agents, informants, investigators, or interrogators.

On February 27, 2013, DoD Instruction (DoDI) 3025.21, "Defense Support of Civilian Law Enforcement Agencies," rescinded DoDD 5525.5, expanding on the existing restrictions and added further restrictions prohibiting DoD personnel from:

- engaging in interviews, interrogations, canvassing, or questioning of potential witnesses or suspects or similar activity;
- using force or physical violence, brandishing a weapon, discharging or using a weapon, or threatening to discharge or use a weapon except in self-defense, in defense of other DoD persons in the vicinity, or in defense of non-DoD persons;
- evidence collection, security functions, crowd and traffic control, and operating, manning, or staffing checkpoints;
- surveillance or pursuit of vehicles, items, transaction, or physical locations; and
- forensic investigations or other testing of evidence obtained from a suspect for use in a civilian law enforcement investigation in the United States unless there is a DoD nexus.

However, DoDI 3025.21 recognizes an exception to the general prohibition on direct involvement when there is an independent military purpose. That is, when military participation is undertaken for the primary purpose of furthering a military or foreign affairs function of the United States, regardless of incidental benefits to civilian authorities. The Instruction details the activities that DoD personnel may undertake to directly assist civilian law enforcement agencies. DoD personnel may participate in:[1]

- investigations and other actions related to enforcing the Uniform Code of Military Justice;
- investigations and other actions that are likely to result in administrative proceedings by DoD, regardless of whether there is a related civil or criminal proceeding; and
- investigations and other actions associated with a commander's inherent authority to maintain law and order on a DoD installation or facility.

While DoDI 3025.21 does not articulate a clear standard where DoD personnel may participate in investigations and other actions in reliance on the independent military purpose exception, the *Dreyer* decision now provides that guidance.

[1] This is not a comprehensive list of all categories of permissible active participation in direct law enforcement-type activities, merely the ones most likely to be applicable to the narrow categories of investigations that are the subject of this evaluation. A complete listing of permissible active participation in direct law enforcement-type activities can be found in DoDI 3025.21, enclosure 3, paragraph 1.b.

Air Force and AFOSI Policy

Air Force (AF) Policy Directive 71-1, "Criminal Investigations and Counterintelligence," January 6, 2010, (Incorporating Change 3, September 30, 2011[2]) states that the AF must collaborate effectively and practically with civilian law enforcement officials while complying with the Posse Comitatus Act. The Directive is intended to provide a framework for conducting criminal and counterintelligence operations and does not offer specific guidance for conducting Internet operations.

Subsequent to the initial *Dreyer* decision, AFOSI published investigative policy to provide guidance and clarity regarding the prohibitions contained in DoDI 3025.21. The interim change to AFOSI Manual (AFOSIMAN) 71-122, "Criminal Investigations," volume 1, September 28, 2012, addressed AFOSI's participation in ICAC operations. Before publication of the interim change, AFOSIMAN 71-122 did not address Internet operations. Therefore, AFOSI did not have guidance addressing its participation in ICAC operations and did not have the reasonable likelihood standard by which the agents must adhere to. The new policy, issued in September 2012, requires AFOSI field units to establish a memorandum of understanding (MOU) with the ICAC Task Force. The policy also states that AFOSI special agents "may only participate in investigations where targets have a military affiliation." The policy further states that online undercover operations conducted by an AFOSI agent will be conducted in accordance with AFOSIMAN 71-118, "Undercover Operations," volume 3, November 13, 2009 (Certified Current December 6, 2011).

AFOSI also published its investigative support guide titled, "Internet Crimes Against Children (ICAC) Operations and Investigations Guide," on February 4, 2015, while our evaluation was ongoing. The investigations we reviewed were conducted before the Guide was published. However, the Guide now provides special agents and supervisors an overview of the typical operations conducted. It also provides detailed instructions for documenting and conducting these investigations. The Guide requires field units to establish that the subject has a "reasonable likelihood of military affiliation" before they initiate investigative action.

[2] A revision of AF Policy Directive 71-1 was published on November 13, 2015.

Finding

Prohibited Investigative Activities

AFOSI lacked specific policy addressing its special agents' roles during ICAC operations, which contributed to violations of the provisions in DoDD 5525.5 and its revised version, DoDI 3025.21. These violations were the result of AFOSI special agents participating in prohibited investigative activities with civilian law enforcement agencies while conducting Internet-based investigations. During the course of our evaluation, AFOSI published investigative policy, which incorporated the reasonable likelihood standard. In addition, DoDI 3025.21 has not been updated to include the reasonable likelihood standard articulated in *Dreyer*.

~~(FOUO-LES)~~ Results of Internet-Based Investigations

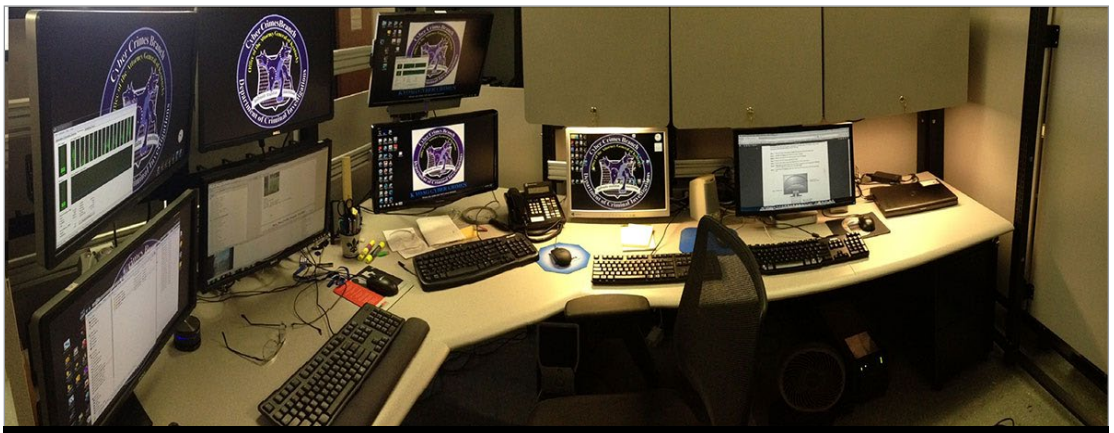

Figure 2. Cyber Crimes Workstation
Source: http://ag.ky.gov/criminal/dci/cybercrimes/Pages/default.aspx

We evaluated two types of Internet-based investigations: (1) P2P file transfer of computer files containing child pornography and (2) solicitation of a minor for sexual purposes. A P2P network is a group of computers that act as a connection point or a redistribution point for file sharing within a peer-networking group. Users must "join" a network to download or share files. The users are informed

that files will be shared once they have joined the network. P2P networks allow each individual computer to act as an independent network server. Within a network, the peer (or computer) portrays the role of both the client and the server at the same time. This means that a peer can initiate requests to other peers and simultaneously respond to incoming requests from other peers within the network.[3]

~~(FOUO-LES)~~ [redacted]

Although both P2P file transfer and solicitation of a minor investigations are examples of Internet-based investigations, such investigations are initiated and investigated differently. Therefore, this evaluation discusses and presents the results of each of these separately.

We evaluated 80 AFOSI Internet-based crime investigations[4] conducted from January 2010 through October 2014. The majority of deficiencies identified in the following sections were the result of AFOSI conducting investigative steps without first establishing the reasonable likelihood of the subject's military affiliation. During our evaluation, AFOSI published policy requiring special agents to establish a reasonable likelihood of military affiliation before undertaking investigative activities and inform ICAC participants and prosecutors of this requirement.

Inherent in the decision to initiate any investigation is a determination that the MCIO has investigative jurisdiction over the crime or subject. Any such initial decision regarding investigative jurisdiction is always subject to reconsideration as additional facts are developed.

[3] For further information on P2P networks, visit http://www.computerworld.com/article/2588287/networking/peer-to-peer-network.html.

[4] Investigative sufficiency was not within the scope of our evaluation and was not evaluated.

DoD Policy Analysis

DoDI 3025.21, which was published on February 27, 2013, has not been updated to discuss the reasonable likelihood standard articulated in the September 2014 *Dreyer* opinion. The current policy focuses on the exceptions when the MCIOs can conduct investigations, but does not focus on how to ensure investigative activity is within the scope of the "independent military purpose" exception. While we focused our review on Air Force policy, we believe including a standard interpretation of the reasonable likelihood standard within DoDI 3025.21 would benefit all MCIOs.

Case Analysis

In reviewing the following cases, we applied a reasonable likelihood of a military affiliation standard, which the *Dreyer* holding introduced. An investigative deficiency is any instance when an investigative step (for example, obtaining a subpoena or conducting an interview) was performed before AFOSI demonstrated there was a reasonable likelihood of the subject's military affiliation. Of the 80 cases evaluated, 57 cases (71 percent) had no deficiencies. The remaining 23 cases (29 percent) had 1 or more deficiencies; that is, violations of DoDD 5525.5/DoDI 3025.21. There was no case file documentation to support a conclusion by AFOSI that there was a reasonable likelihood of the subject's military affiliation in the 23 cases with deficiencies. Table 1 reflects a breakdown of the types of cases, the number of cases evaluated, and the number of cases with and without deficiencies.[5] Examples of the deficiencies are provided in the following sections.

Table 1. Internet-Based Cases from FY 2010 through FY 2014

Internet-Based Cases	Total	Cases with Deficiencies	Cases without Deficiencies
P2P Cases	48	15	33
Solicitation Cases	30	8	22
Other Cases*	2	0	2
Total Cases Evaluated	**80**	**23**	**57**

* Other cases involved Internet-based behavior other than P2P or solicitation of a minor.

[5] Table 1 numbers include three unknown subject cases (one solicitation and two P2P). For the purpose of analysis, we classified the unknown subjects as "civilians" because we could not determine their DoD military affiliation.

Analysis of Investigative Deficiencies

We analyzed the combined data related to deficiencies in the 23 cases evaluated. Our analysis disclosed deficiencies that included: 1) gathering of evidence, 2) obtaining a subpoena, 3) conducting undercover operations, and 4) conducting surveillance.

Table 2 reflects a breakdown of the cases by type and whether the subject of the investigation was eventually determined to be DoD military affiliated or a civilian.

Table 2. Cases with Civilian Subjects and Military Subjects

Internet-Based Cases	Cases with Deficiencies	Cases with Civilian Subjects	Cases with Military Subjects
P2P Cases	15	8	7
Solicitation Cases	8	5	3
Total Cases with Deficiencies	**23**	**13**	**10**

Deficiency Related to the Collecting of Evidence

Of the 23 cases with deficiencies, 1 (4 percent) had a deficiency related to the collecting of evidence. AFOSI collected evidence (a digital shared file suspected of containing child pornography) in a P2P case before establishing the potential subject had a reasonable likelihood of a military affiliation.

Subpoena Deficiencies

~~(FOUO-LES)~~ [redacted]

P2P Subpoena Deficiencies

~~(FOUO-LES)~~ In four P2P cases, non-DoD OIG subpoenas were served before AFOSI knew the identities of the subjects and before establishing the potential subjects had a reasonable likelihood of a military affiliation. [redacted]

[6] [redacted]

Solicitation of a Minor Subpoena Deficiencies

In one case, a subpoena was served before AFOSI knew the identity of the subject and before establishing the potential subject had a reasonable likelihood of a military affiliation.

Undercover Deficiencies

~~(FOUO-LES)~~ Of the 23 cases with deficiencies, 20 (87 percent) had undercover deficiencies. [redacted]

P2P Undercover Deficiencies

~~(FOUO-LES)~~ [redacted]

Solicitation of a Minor Undercover Deficiencies

~~(FOUO-LES)~~ In 19 cases, AFOSI initiated undercover operations against a subject without first establishing there was a reasonable likelihood of the subject's military affiliation. [redacted]

~~(FOUO-LES)~~ Furthermore, in 3 of the 19 deficient solicitation of a minor cases, [redacted]

Surveillance Deficiencies

Of the 23 cases with deficiencies, 17 (74 percent) had surveillance deficiencies. There were no surveillance deficiencies noted in solicitation of a minor cases.

P2P Surveillance Deficiencies

~~(FOUO-LES)~~ [redacted]

[7] ~~(FOUO-LES)~~ [redacted]

~~(FOUO-LES)~~ [redacted]

Conclusion

In the deficient cases, before establishing a reasonable likelihood of the subject's military affiliation, AFOSI violated DoDD 5525.5 or DoDI 3025.21 by providing various prohibited forms of direct civilian law enforcement assistance. The deficiencies included:

- collection of evidence,
- obtaining subpoenas,
- conducting undercover operations, and
- conducting surveillance.

Even though AFOSI was part of the ICAC task force, it should have ensured there was a reasonable likelihood of the subject's military affiliation before participating in the investigation.

We determined the reason for these deficiencies was, in part, the lack of AFOSI policy addressing its investigative role during ICAC operations. During our evaluation, AFOSI published an "Internet Crimes Against Children (ICAC) Operations and Investigations Guide" February 4, 2015,[8] and a policy change to AFOSIMAN 71-122, volume 1, to alleviate future violations. These policies are consistent with the 9th Circuit's interpretation of DoDI 3025.21 and the Posse Comitatus Act in the *Dreyer* case. As such, we are not making any recommendations to AFOSI at this time.

Recommendation, Management Comments, and Our Response

We recommend that the Under Secretary of Defense for Policy (USD(P)) clarify DoD Instruction 3025.21, "Defense Support of Civilian Law Enforcement Agencies," Enclosure 3, "Participation of DoD Personnel in Civilian Law Enforcement Activities," to reflect the holding in *United States v. Dreyer*, 767 F.3d 826, affirmed in relevant part by 2015 U.S. App. LEXIS 19226 (9th Cir., *en banc*).

[8] The Guide is instructional in nature and is not compulsory.

Under Secretary of Defense for Policy Comments

The Director, Defense Support of Civil Authorities, responding for the Under Secretary of Defense for Policy, stated that his initial assessment of our evaluation and the *U.S. v. Dreyer* decision was that the relevant provisions of DoDI 3025.21, enclosure 3, provide sufficient clarity to MCIOs to have avoided the outcome in *U.S. v. Dreyer.* However, having reconsidered his initial assessment, he agreed with our recommendation to clarify DoDI 3025.21, enclosure 3, when the Instruction is revised in 2017 to reflect the holding in *Dreyer*.

The Director also stated that in the case of *Dreyer,* a properly trained NCIS agent knew, or should have known, that his activities were in violation of the DoDI, as written. The Director contended that the violation in *Dreyer* appeared to be more of an education and training issue than a policy issue.

Our Response

The Director, Defense Support of Civil Authorities, responding for the Under Secretary of Defense for Policy, agreed with our recommendation to clarify DoDI 3025.21, however, he did not fully agree with our conclusion that the policy needed to be updated. He opined that the Dreyer violation was more an education and training issue than a policy issue. We disagree. We believe if the violation was a single, isolated violation, it could be considered solely an education and training issue. However, our comprehensive review of AFOSI internet operations determined that the numerous violations we identified clearly indicate a lack of clarity in DoDI 3025.21.

We appreciate the Director's reconsideration of his initial assessment of our recommendation to clarify the policy and we agree that additional training and education would help address the issues identified in this report. Training and education could serve to mitigate any confusion related to the policy between now and 2017, when the Director indicated DoDI 3025.21 would be updated. The Director, Defense Support of Civil Authorities, should work with the MCIOs to develop an education and training program that ensures special agents properly employ the requirements in DoDI 3025.21. While we find the Director's comments responsive to our recommendation, we request that the Under Secretary of Defense for Policy provide comments to this final report that address his plans to work with the MCIOs on developing an education and training program and when that will occur.

Observation

AFOSI Policy

At the time of the evaluation, AFOSI policy[9] did not define special agents' roles and responsibilities regarding Internet-based operations, nor did it require the execution of MOUs for participation in ICAC task forces.

Discussion

In response to our data call, AFOSI provided its applicable policy and regulatory guidance governing Internet-based operations. We analyzed applicable guidance and discovered AFOSI policy did not define special agents' roles and responsibilities regarding Internet-based operations or their participation in ICAC task forces. Throughout our evaluation, we reviewed some AFOSI case files that contained examples of prohibited forms of direct civilian law enforcement assistance, which violated DoDD 5525.5 or DoDI 3025.21.

We reviewed 15 MOUs[10] established between AFOSI and civilian law enforcement organizations. Nine of the 15 MOUs lacked specifics as to AFOSI's roles, responsibilities, and prohibitions relative to Posse Comitatus. The other six minimally addressed AFOSI's roles, responsibilities, and prohibitions relative to Posse Comitatus.

Conclusion

When AFOSI conducted the investigations, it did not have sufficient policy and guidance, such as MOUs, to govern Internet-based operations. However, during our evaluation, AFOSI published interim change to AFOSIMAN 71-122, volume 1 addressing the prohibitions in DoDI 3025.21 and the need for MOUs. Additionally, as stated in the Finding section, AFOSI published the "ICAC Operations and Investigations Guide." The Guide addresses both P2P and solicitation of a minor (chat) investigations and the language of the Guide supports actions that are in compliance with the Posse Comitatus Act and DoDI 3025.21. In addition, the Guide includes the need for MOUs and the "reasonable likelihood of military affiliation" standard contained in *Dreyer*.

[9] During the evaluation, AFOSI published policy governing special agents' participation in ICAC operations.
[10] For this report, the term "MOU" will also include any MOAs.

Appendix

Scope and Methodology

We conducted this evaluation in accordance with the Council of Inspectors General on Integrity and Efficiency, "Quality Standards for Inspections and Evaluations," January 2012. Based on the assessment objectives, we planned and performed the evaluation to obtain sufficient evidence to provide a reasonable basis for our observations and conclusions.

Our evaluation began with a review of AFOSI's policies and procedures guiding its compliance with Federal statutes and DoD policy regarding Posse Comitatus, Internet-based operations, and undercover operations. We then evaluated how AFOSI ensures its special agents' compliance with those policies and procedures.

We developed a case review protocol based on AFOSI's policies and procedures governing Internet-based operations, MOUs, and undercover operations from January 2010 through October 2014. We used the protocol to review Internet-based investigations for compliance with applicable policy and guidance. We also reviewed the applicable ICAC task force MOUs that AFOSI provided us and recorded the results on an Excel spreadsheet instead of a database due to the limited number of data points to be collected.

We determined there were seven cases that did not meet the scope of the evaluation; for example, cases opened before CY 2010, cases where the initial investigative work was completed by an agency other than AFOSI, or the crime was not perpetrated online. We also excluded 42 target management files because they are used to document broad efforts against a specific target and do not contain enough information to initiate an investigation.

Quality Assurance

To ensure consistent application of evaluation methodology, the project manager and team leader performed quality assurance reviews on a random number of the evaluation sample cases. The quality assurance reviews consisted of the project manager or team leader conducting a full review of the case and matching those results to the results of the initial review. There were no differences discovered during the quality assurance reviews.

Data Analysis and Deficiencies Analysis

Our case review protocol allowed us to place case information in a database. At the conclusion of the case evaluation phase, we analyzed the data collected and stored in the database through numerous queries designed to efficiently identify specific investigative tasks and steps that were completed by AFOSI special agents. The queries indicated what tasks or investigative steps were involved with each deficiency and the number of instances of each. We reviewed the statistical percentages of the investigative tasks identified and determined if they were successfully completed before or after it was determined there was a reasonable likelihood the subject had a military affiliation.

The DoD OIG Office of General Counsel reviewed the laws and implementing guidance applicable to our evaluation and provided guidance for a standard that we used to determine deficiencies.

Use of Computer-Processed Data

We used computer-processed data to perform this evaluation as detailed in the preceding data analysis and deficiency analysis section. AFOSI personnel provided data obtained from their Investigative Information Management System (I2MS). The data identified the number of cases, subjects, and investigative steps taken during the investigation. This information was provided in Excel spreadsheets.

We tested the reliability of the data during our site visits to AFOSI Headquarters. Specifically, we validated the information provided with the review of the hard copy case files and our review of I2MS itself.

We used all other computer-processed data for contextual purposes; therefore, we determined the data was sufficiently reliable for our purposes.

Prior Coverage

No prior coverage has been conducted on AFOSI Internet-based operations during the last 5 years.

Management Comments

Under Secretary of Defense for Policy Comments

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE
2600 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-2600

HOMELAND DEFENSE & GLOBAL SECURITY

MAR 2 3 2016

SSA [redacted]
Office of the Inspector General
Department of Defense
4800 Mark Center Drive
Alexandria, VA 22350-1500

Dear SSA [redacted]

Thank you for the opportunity to review the Draft DoD IG report "Evaluation of the Air Force Office of Special Investigations' Conduct of Internet-Based Operations and Investigations (Project No. 2014C018)."

I've reviewed both the Draft report and U.S. v. Dreyer, 767 F.2d 826 (9th Cir., 2014). I concur with comments to the IG's draft recommendation that USDP "clarify DoD Instruction 3025.21, enclosure 3, to reflect the holding in U.S. v. Dreyer [where the 9th Cir.] established a standard requiring a reasonable likelihood of a subject's military affiliation before Military Criminal Investigative Organizations (MCIOs) conduct investigative activities."

My initial assessment, from my reading of both the draft report and the Dreyer decision, is that the relevant provisions of DoDI 3025.21, enclosure 3, provide sufficient clarity to MCIOs to have avoided the outcome in Dreyer.

A properly trained NCIS agent, in my view, knew, or should have known, that his activities were in violation of the DoDI, as written. The 9th Circuit discussed the relevant DoD policies in detail and did not suggest that either the SecNav or DoD guidance was inadequate. I contend that this appears to be more of an education and training issue than a policy issue.

Given the extensive evaluation your office did reviewing Air Force Office of Special Investigations' conduct of internet-based operations and investigations, it appears that more clarification may be necessary. I appreciate your office adding clarification to DoDI 5505.03 (Initiation of Investigations by Defense Criminal Investigative Organizations). My office will include similar clarification when we revise DoDI 3025.21 (Defense Support of Civilian Law Enforcement Agencies) sometime in 2017.

[redacted]
Director, Defense Support of Civil Authorities

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

Acronyms and Abbreviations

AF	Air Force
AFOSI	Air Force Office of Special Investigations
AFOSIMAN	Air Force Office of Special Investigations Manual
ICAC	Internet Crimes Against Children
MCIO	Military Criminal Investigative Organization
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
NCIS	Naval Criminal Investigative Service
OIG	Office of Inspector General
P2P	Peer-to-Peer
U.S.C.	United States Code


INSPECTOR GENERAL
INTEGRITY
EFFICIENCY
DEPARTMENT OF DEFENSE

Whistleblower Protection
U.S. Department of Defense

The Whistleblower Protection Enhancement Act of 2012 requires the Inspector General to designate a Whistleblower Protection Ombudsman to educate agency employees about prohibitions on retaliation, and rights and remedies against retaliation for protected disclosures. The designated ombudsman is the DoD Hotline Director. For more information on your rights and remedies against retaliation, visit www.dodig.mil/programs/whistleblower.

For more information about DoD IG reports or activities, please contact us:

Congressional Liaison
congressional@dodig.mil; 703.604.8324

Media Contact
public.affairs@dodig.mil; 703.604.8324

For Report Notifications
http://www.dodig.mil/pubs/email_update.cfm

Twitter
twitter.com/DoD_IG

DoD Hotline
dodig.mil/hotline

DEPARTMENT OF DEFENSE | INSPECTOR GENERAL

4800 Mark Center Drive
Alexandria, VA 22350-1500
www.dodig.mil
Defense Hotline 1.800.424.9098